INTERNET ACCESS, INTERNET SAFETY, PERSONALLY OWNED DEVICES, AND USE OF ELECTRONIC RESOURCES

Student Internet Access Agreement: Students and their parent or guardian must sign a Student Internet Access Agreement in order to use the Internet and access the BYOD (Bring Your Own Device) network. A parent can withdraw approval at any time.

The District maintains the right to place reasonable restrictions on the material accessed or posted through District networks. The District's networks are considered a limited forum, similar to the school newspaper, and therefore the District may impose restrictions for valid educational reasons.

Acceptable Uses: The District's networks and the Internet may be used for activities resulting from specific tasks and assignments which support learning and teaching, and which promote the District's mission and goals. Students bear the burden of responsibility to inquire with school administrators and/or teachers when they are unsure of the permissibility of a particular use of technology prior to engaging in the use. Students and employees are to use the system only for educational activities, administrative activities, and academic research.

Prohibited Uses: Prohibited uses are those which violate an individual's right to privacy or access to materials, information, or files of another individual or organization without permission; violation of copyright laws or software licensing agreements; those which spread computer viruses; deliberately attempt to vandalize, damage, disable, or disrupt the property of the District, another individual or individual, organization, or the network; or any effort to locate, receive, transmit, store, or print files or messages that are profane, which depict nudity, sex, sexual acts, excretion, and exhibition of genitals, or use language that is offensive or degrading to others.

1. Students and employees may not use the District's networks and the Internet for commercial purposes that result in personal gain. Students and employees may not offer, provide, or purchase products or services through the Putnam City School District networks and the Internet unless authorized by the Administration, Board or Board policies and regulations.

2. Students and employees may not use District's networks and the Internet for political lobbying. Students and employees may use the system to communicate with elected representatives and to express their opinions on political issues.

3. Students and employees will not attempt to gain unauthorized access to the District's networks or to any other computer system through the district networks, or go beyond individual authorized access. This includes attempting to log in through another person's user name or accessing another person's files. These actions are prohibited, even if only for the purposes of "browsing".

4. Students and employees will not make deliberate attempts to disrupt the computer system or destroy data by spreading computer viruses or by any other means.

5. When instances of use outside of school carry over to the school day in a way that disrupts the instructional process and the learning environment, the school is empowered to deal with the disruption in a disciplinary action.

6. Social networking websites are a popular method of communication among students and employees in the off-campus hours. When off-campus use carries over to the school day in a way that disrupts the instructional process and the learning environment, the school is empowered to deal with the disruption in a disciplinary action.

7. Personally and District owned devices are permitted for educational purposes and/or in approved locations only. The use of personally owned devices in locker rooms, restrooms, and nurses' offices is prohibited.

8. Students are not permitted to use any electronic device to record audio or video media or take pictures of any student or staff member without their permission. The distribution of any unauthorized media may result in discipline including suspension or criminal charges.

Personally Owned Devices: All district students shall review and agree to this policy before connecting any personally owned device(s). The District reserves the right to restrict student use of district owned technologies and personally owned devices on school property or at school-sponsored events. Students who disrupt the safety and/or well-being of the school are subject to disciplinary action.

A personally owned device will include all existing and emerging technology devices that can take photographs; record audio or video; input text; upload and download media; and transmit or receive messages or images. Examples of a personally owned device shall include but is not limited to: MP3 players and iPods; iPads, Nooks, Kindle, and other tablet PCs; laptop and netbooks computers; personal digital assistants (PDAs), cell phones and smart phones such as BlackBerry, iPhone or Android, as well as any device with similar capabilities.

The student network is made available as a resource. The District may block or remove student access if deemed necessary. All personal devices accessing the Internet through the District network will be subject to the District's content filtering system. Students are responsible for all content accessed from their device.

Not all devices may be compatible with the network authentication system. Devices must be able to securely connect to an 802.1x-enabled network.

Students and employees joining the District network with personal devices will self-register their devices and those devices will be electronically tied to that person for a set time period. Students and staff may be limited on registering the number of concurrent devices.

The District shall not be liable for the loss, damage, misuse, theft of any personally owned device brought to school.

The District reserves the right to monitor, inspect, copy, and review a personally owned device or file when administration has a reasonable suspicion that a violation has occurred.

Obeying the Law: Students and employees are responsible for respecting and adhering to local, state, and international laws governing use of information and the available technologies.

Violations: Any attempt to violate the guidelines for use of technology, the network, or the Internet, may result in revocation of user privileges, and/or other disciplinary actions consistent with Board of Education Policy.

Personal Storage Devices: The teacher in charge may disallow the use of personal storage devices on network computers.

Inappropriate Communication: Inappropriate communication includes, but is not limited to: obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted or spoken by students; information that could cause damage to an individual or the school community or create the danger of harassment (persistently acting in a manner that distresses another person) or stalking of others; knowingly or recklessly posting false or defamatory information about a person or organization; and communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices. If a student or employee is told to stop sending communications, they must cease the activity immediately.

Appropriate Language: Language typed, printed, and/or sent will be appropriate at all times.

1. Restrictions against inappropriate language apply to public messages, private messages, and material posted or viewed on web pages.

2. Students and employees will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.

3. Students and employees will not engage in personal attacks, including prejudicial or discriminatory attacks.

4. All communication will be courteous.

Personal Safety: Personal addresses and phone numbers are not to be given to strangers on the Internet. Students and employees should not post personal contact information about themselves or other people.

The educational use of social networking sites, blogs, chat rooms, and other electronic interactions can be a positive experience for students and employees, but if they are not used safely, can be a damaging experience. Everyone is encouraged to be aware of the dangers in providing personal information on social networking sites, blogs, chat rooms, emails, or instant messages. Users should choose carefully whether or not to make their profile on social networking sites publicly viewable and available, or to keep it private and limited to the friends of their choosing.

Personal contact information includes addresses, telephone numbers, school addresses, work addresses, etc. Students will promptly disclose to their teacher, library media specialist, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.

Students and employees will not use "non-educational" chat rooms, blogs, social networking sites, and instant messaging programs at school or in the workplace on district hardware.

The District will provide instruction about appropriate online behavior, including interacting with other individuals on social networking web sites and chat rooms. Additionally, cyberbullying awareness and response will be taught annually.

Individual Student and Employee Privacy and the Privacy of Others: Electronic mail will not be private; system administrators will have access to all mail. Files stored on school-based computers will not be private. Administrators and staff members may review files and messages to maintain system integrity and ensure that users are acting in a responsible manner.

1. Students and employees should expect only limited privacy in the contents of personal files on district networks. The situation is similar to the rights students have in the privacy of their lockers.

2. Students and employees will not re-post a message that was sent to them privately without permission of the person who sent the message.

3. Students and employees will not post private information about another person.

4. Students and employees will not infringe upon another's folders, work, or files.

Inappropriate E-mail: Inappropriate e-mail and other electronic documents transmitted on district networks or shared on electronic devices prohibited at school will be forwarded to the designated administrator for processing and disciplinary action.

Security: Measures taken to ensure security shall be respected.

Property Rights: All information accessible via the network is assumed to be private property; copyright statutes apply.

1. Students and employees will not plagiarize works that are found on the Internet.

2. Students and employees will respect the rights of copyright owners and licensing agreements. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. If a work contains language that specifies appropriate use of that work, the expressed requirements must be followed. If unsure how a work can be used, permission should be requested from the copyright owner. Copyright law can be very confusing. Questions should be directed to the teacher or library media specialist.

Reporting of Violations: Any violation of the guidelines for use of the network and/or the Internet should be reported to the teacher or library media specialist in charge.

Employees will notify their principal or supervisor of any message they receive, or activity they observe, that is inappropriate or makes them feel uncomfortable.